Summary In this chapter, you've learned about the foundations of managed services, including mapping cloud provider and customer responsibilities in the three most common models of cloud computing. We explored how communications are secured, including through the use of encryption, and how infrastructure is protected using a variety of security techniques like network security groups, traffic inspection, geofencing, and zero trust. We also looked at common network security tools like firewalls, IDSs and IPSs, honeypots, vulnerability scanning, and bastion hosts, which can all be used to help secure your infrastructure. Hardware security devices like HSMs and TPMs also play a role by keeping secrets secure and helping with encryption throughout cloud environments. Verifying that the software you use is secure and trustworthy is an important part of any environment, but code- defined systems like those found in cloud environments are often even more dynamic. That means that you need to know how to manage the software your organization uses and how to validate the packages and components that are in use. The security of virtual environments, including virtual machines and containers, is critical to a cloud environment. We dug into how network, storage, memory, processors, hypervisors, operating systems, and virtualization toolsets all play a role in ensuring security in cloud services. Cloud environments, much like on- premises systems, also require configuration management and hardening. Configuration techniques and practices for both host and guest operating systems, as well as considerations like backups and restoration capabilities, were all topics we reviewed in this chapter. Identity assurance— making sure users are who they say they are and validating their usage of services and systems throughout a cloud environment— requires special attention in the cloud. Hosted services need to integrate with identity providers, and secrets and key management are important for organization and system security. In this chapter, you learned about the challenges that virtualization and the cloud add in addition to typical identity assurance hurdles. Finally, organizations need to be able to ensure that what they believe is occurring actually is. That's where audits come into play. You should now be familiar with both internal and external audits, how to plan them, and the special considerations that you need to plan for in cloud and hybrid environments. **Exam Essentials Understand how key network security concepts like security groups, traffic inspection, geofencing, and zero trust work in the cloud.** Security in the cloud relies on many of the same concepts and technologies as on- premises infrastructure. Be able to describe security groups and their role as virtual firewalls. Explain why inspection remains useful but often requires use of provider- specific tools or is limited due to limitations on network visibility in the virtualized environment. Describe the role of geofencing and limitations on where in a provider's infrastructure activities can take place or which regional connections can provide an additional security layer. Explain why zero trust is sometimes easily built in new cloud environments where tooling exists natively to enable it. **Explain cloud infrastructure elements and how they can be secured.** Cloud infrastructure design requires you to understand its capabilities, risks, and limitations. Explain why network communication should be encrypted end to end to prevent potential issues in shared environments. Explain why storage should also be encrypted by default in most environments to prevent attacks on data at rest as well as in transit. Understand that compute is typically a shared resource on underlying hardware, which could present risks if the provider does not effectively isolate customers or a vulnerability is found. Be able to outline how cloud management planes provide control over entire infrastructures and require strong practices and policies like universal multifactor authentication, secrets management, and security policies that are rooted in least privilege with effective monitoring and alerting. Describe key management plane functionality like scheduling, the ability to orchestrate complex systems, and features that make it easier to manage ephemeral and scalable systems. **Explain virtualization security in a cloud environment.** Explain the role of VM management tools as well as security requirements for hardware components in a virtualized environment. Detail how to secure virtual networks, storage, and CPUs. Describe the differences between Type 1 and Type 2 hypervisors. Explain the role and purpose of virtualization toolsets and plug- ins. Explain the common challenges to identity assurance in cloud environments. **Apply best practices to cloud security operations.** Describe hardware security modules (HSMs) and how they are used in cloud environments, including dedicated and

shared modes of use. Explain what a TPM is and its role in securing systems. Explain the role of firewalls, intrusion detection, and prevention systems. Know how to use vulnerability scanning and assessment tools in segmenting traffic, detecting attacks, and finding potential attack vectors and how their deployment may be different in the cloud. Describe the role of bastion hosts in cloud infrastructure. **Use security baselines to protect systems in the cloud.** Describe SOC 1 and SOC 2 Type 1 and Type 2 audits. Explain how to support audit objectives and processes in the cloud as well as how a security practitioner's role may differ in internal and external audits. Detail the basic concepts of audit planning in the cloud.